정수론 HW2

20011759 박수민

n은 15 초과의 소인수를 가지지 못한다 왜냐하면 n이 15를 초과하는 소인수를 가진다면   
 에서 부분에 의해 14를 초과할 수 밖에 없기 때문이다. 그러므로 라 하자. 그러면 은 다음과 같다

이다. 그런데 4,6,10,12에는 어떠한 정수를 곱해도 14를 만들 수 없다. 그러므로 소인수 5,7,11,13을 가지지 못한다. 그러면 형태이고  
이다. 그런데 를 보면 알 수 있듯 14를 만들기 위해서는 는 7을 소인수로 포함하고 있어야 하나 는 소인수를 2, 3만을 가지므로 7를 가지지 못한다. 그러므로 인 자연수 은 존재하지 않는다.

이므로 라 하자.  
우선 이므로 이다.  
이므로 임을 알 수 있다. 이제 임을 보이면 된다.  
그런데 이므로 이다. 이때 이 홀수이므로 가 된다. 이므로 이다.

를 만족하는 소수 가 유한하다 가정하고 이러한 소수의 집합을 라 하자. 라 한다면 은 자명하게 5일 것이다.  
라 한다면 이므로 위 가정에 의해 합성수이다.  
그렇다면 형태로 인수분해가 가능하다는 뜻이 된다.()

에서 의 모든 원소는 홀수이므로 은 홀수이고, 은 홀수이다. 그러므로 n의 임의의 소인수 에 대해, 임을 알 수 있다. (이라면 q는 짝수가 되는데 그러면 n이 짝수가 되기 때문이다.)  
그리고 이라면 임의의 정수 k에 대해(그리고 임의의 정수 에 대해 으로 두면), ), )이므로 q와 곱해지는 수가 짝수라면 법 6에서 0과 합동, 홀수라면 법6에서 3과 합동이다. 즉, 소수 와 임의의 정수 곱은 법 6에서 3 또는 0만 합동이고 이므로 이다. 즉, 이다. 그런데 모든 에 대해 적어도 하나 이상은 이다. 왜냐하면 모든 소인수가 법 6에서 1과 합동이라면 이들의 곱인 또한 법 6에서 1과 합동이기 때문이다. 즉 인 임의의 의 소인수를 라 두자

이고 이므로 이다. 그리고 이고  
이므로 이다. 즉 P의 원소로는 을 나눌 수 없으나 이다. 즉, 인데 이므로 가정과 모순된다. 그러므로 를 만족하는 소수는 무한히 많다.

파이썬을 사용하여 계산하였다.  
def pow\_mod(a,e,m):

if(e == 1):

return a % m;

ebit1 = e % 2;

e=e>>1

return (a\*\*ebit1 % m) \* ((pow\_mod(a,e,m)\*\*2) % m) % m;

n=int(input())

if(n%2==0):

print("ERROR, n must be odd")

exit(0)

tmp = n - 1

k=0

while(tmp % 2 == 0):

k+=1

tmp = tmp >> 1

q = tmp

isComposite = False

for a in range(1,n):

if(pow\_mod(a,q,n) == 1):

continue

check2 = True

for i in range(0,k):

if(pow\_mod(a,q\*(2\*\*i),n)==n-1):

check2 = False

break

if(not check2):

continue

isComposite = True

break

if isComposite:

print("n is composite number")

else :

print("n is not composite number")

텍스트, 스크린샷, 디스플레이, 소프트웨어이(가) 표시된 사진

자동 생성된 설명